09/647961

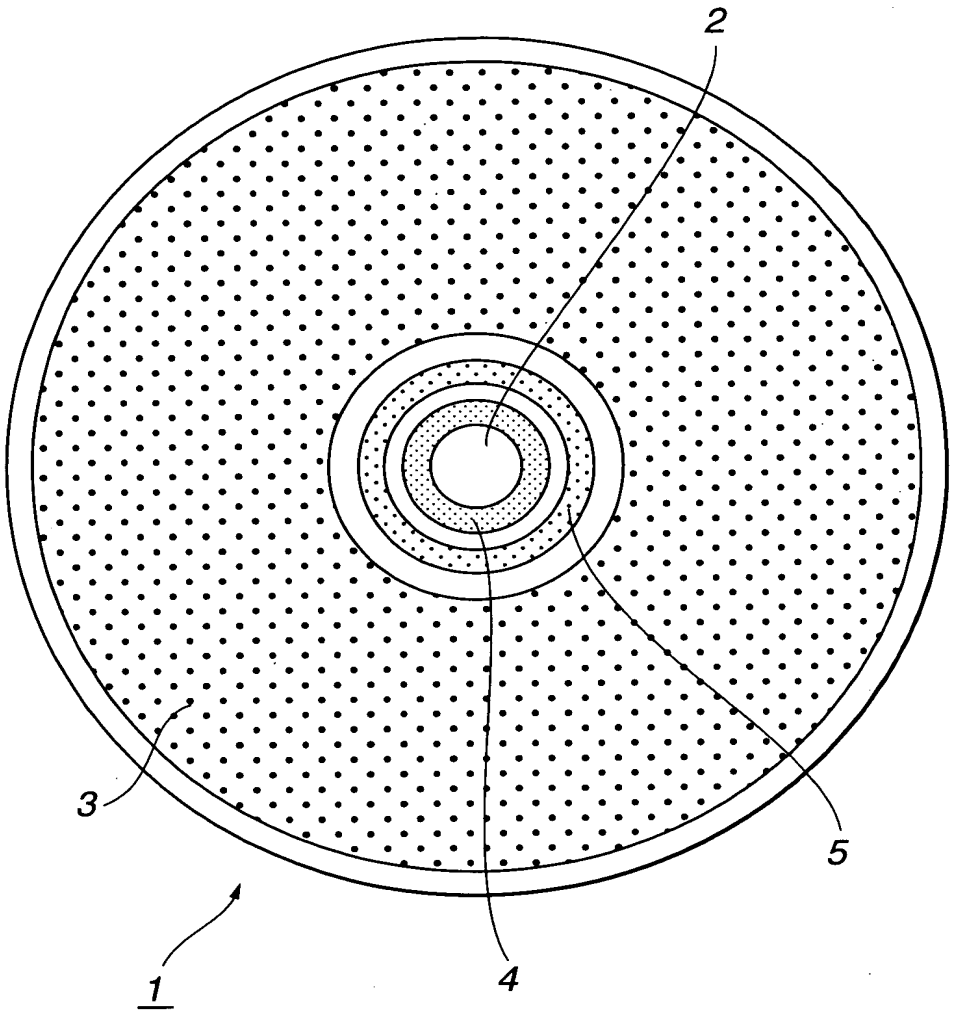

FIG.1

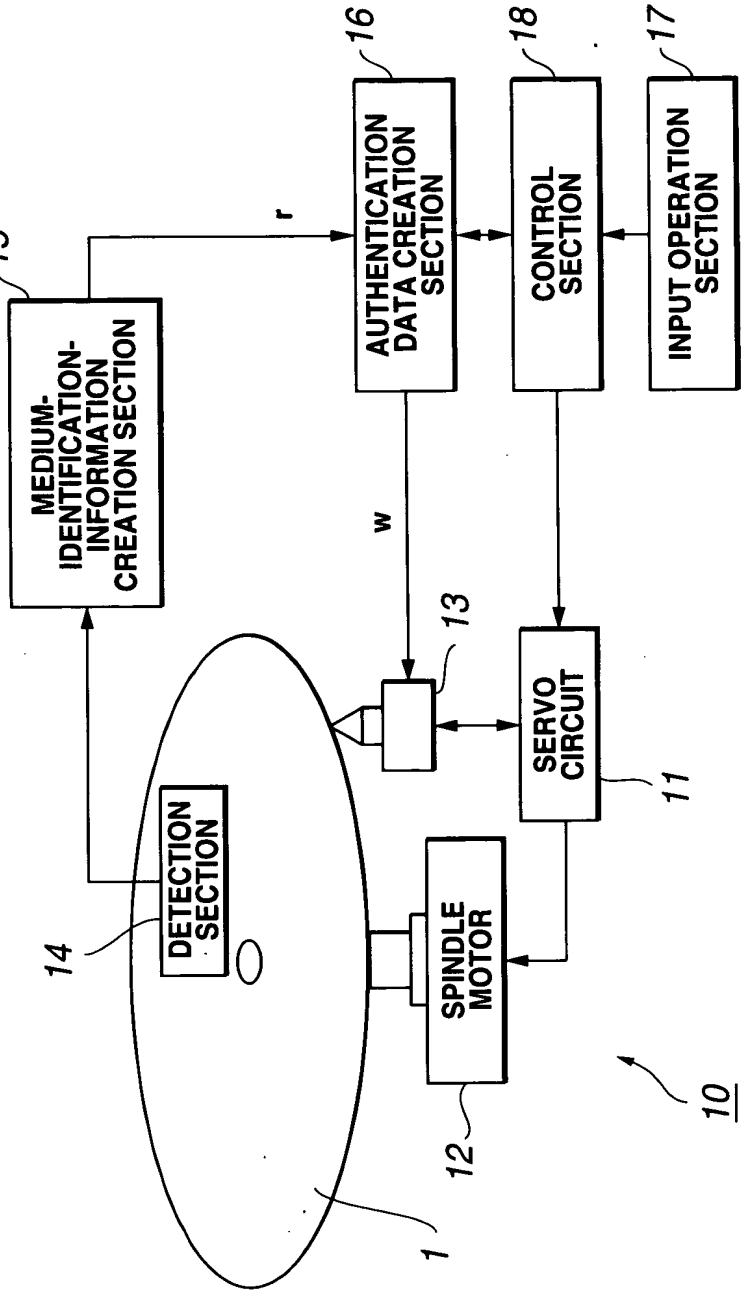
MEDIUM-IDENTIFICATION-INFORMATION CREATION SECTION
15
r
AUTHENTICATION DATA CREATION SECTION
16
CONTROL SECTION
18
INPUT OPERATION SECTION
17
w
13
SERVO CIRCUIT
11
DETECTION SECTION
14
SPINDLE MOTOR
12
1
10

FIG.2

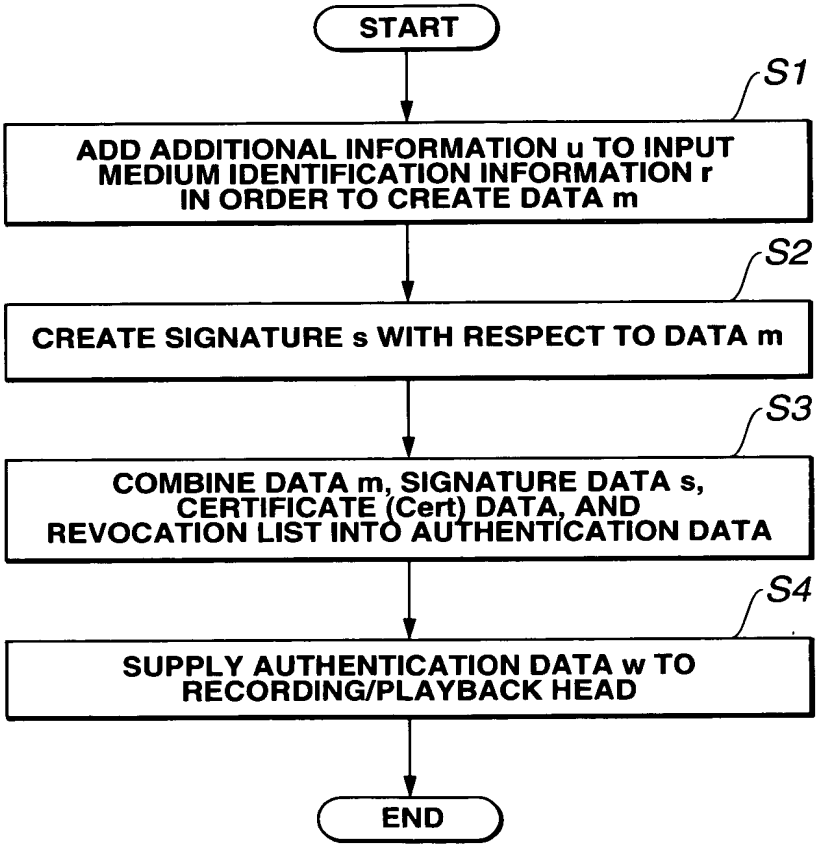
START
S1
ADD ADDITIONAL INFORMATION u TO INPUT MEDIUM IDENTIFICATION INFORMATION r IN ORDER TO CREATE DATA m
S2
CREATE SIGNATURE s WITH RESPECT TO DATA m
S3
COMBINE DATA m, SIGNATURE DATA s, CERTIFICATE (Cert) DATA, AND REVOCATION LIST INTO AUTHENTICATION DATA
S4
SUPPLY AUTHENTICATION DATA w TO RECORDING/PLAYBACK HEAD
END

FIG.3

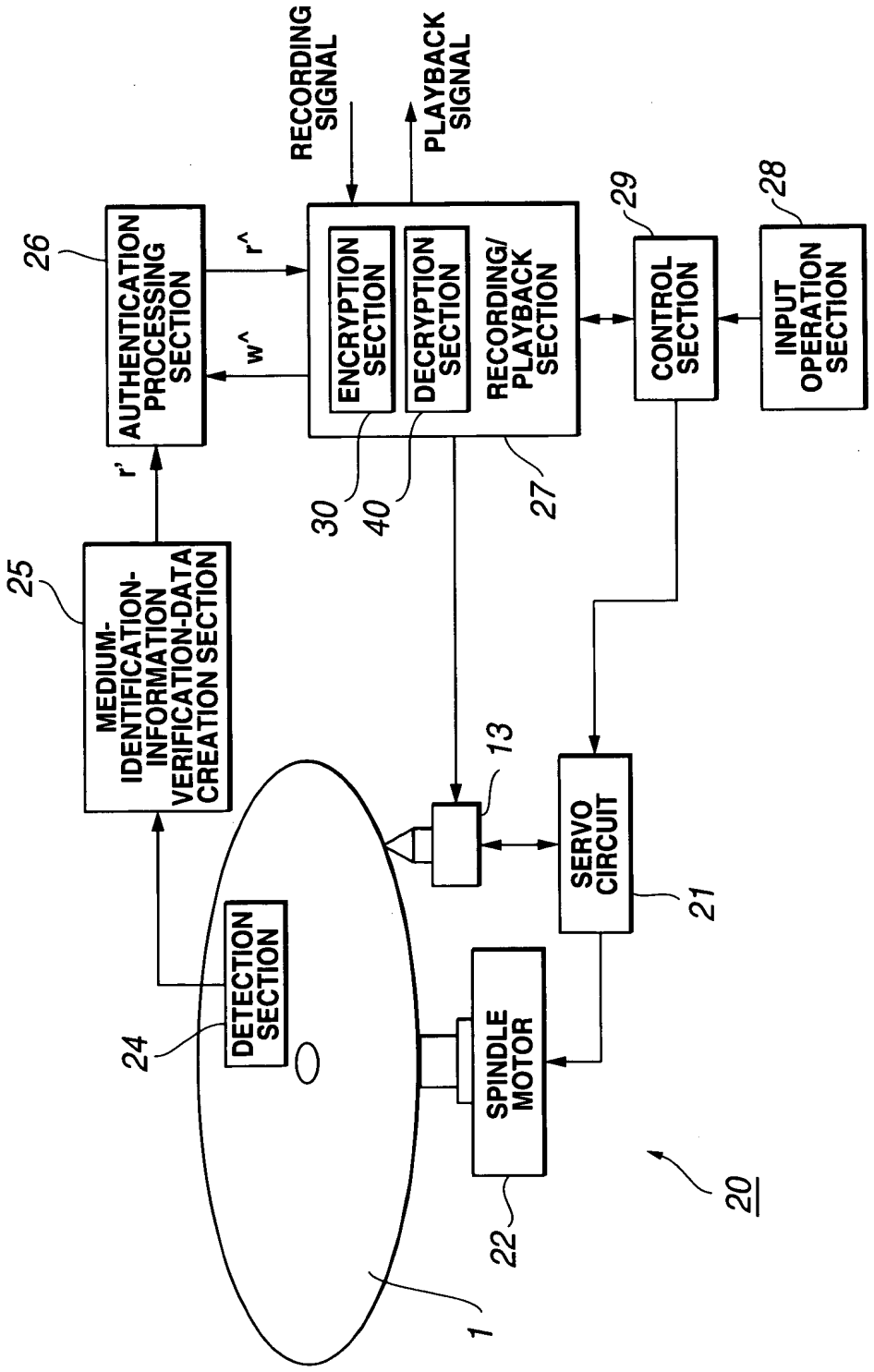
RECORDING SIGNAL
PLAYBACK SIGNAL
26
AUTHENTICATION PROCESSING SECTION
r'
r^
w^
ENCRYPTION SECTION
DECRYPTION SECTION
RECORDING/ PLAYBACK SECTION
29
CONTROL SECTION
28
INPUT OPERATION SECTION
30
40
27
25
MEDIUM-IDENTIFICATION-INFORMATION-VERIFICATION-DATA CREATION SECTION
13
SERVO CIRCUIT
21
DETECTION SECTION
24
SPINDLE MOTOR
22
1
20

FIG.4

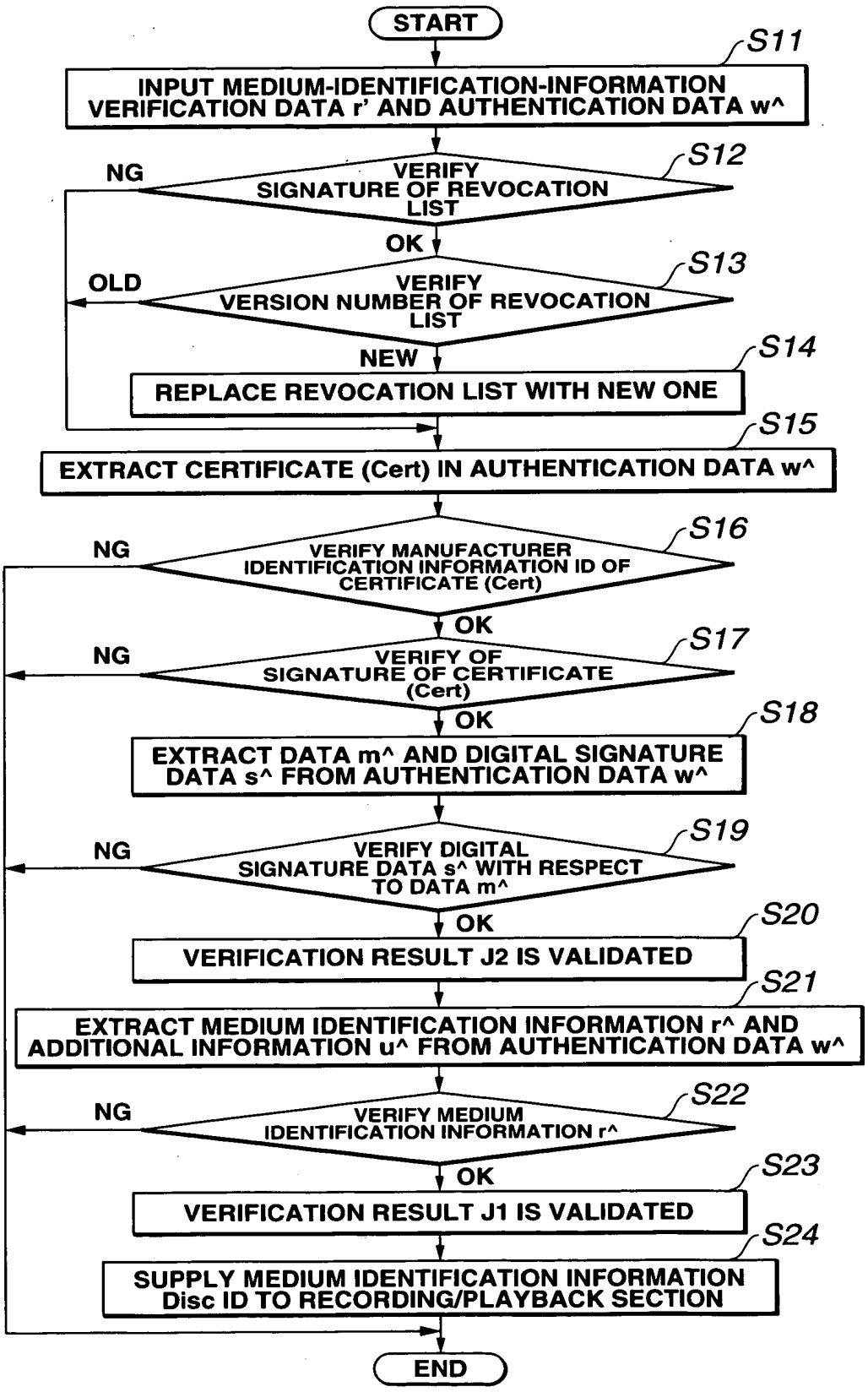

FIG.5

09647961 - 090204

REVOCATION LIST

VERSION NUMBER
MANUFACTURER ID
. . .

FIG.6

PUBLIC KEY LIST

VERSION NUMBER OF LATEST REVOCATION LIST		
MANUFACTURER ID	PUBLIC KEY	REVOCATION FLAG (YES/NO)
. . .	. . .	. . .

FIG.7

09271-P50459-00

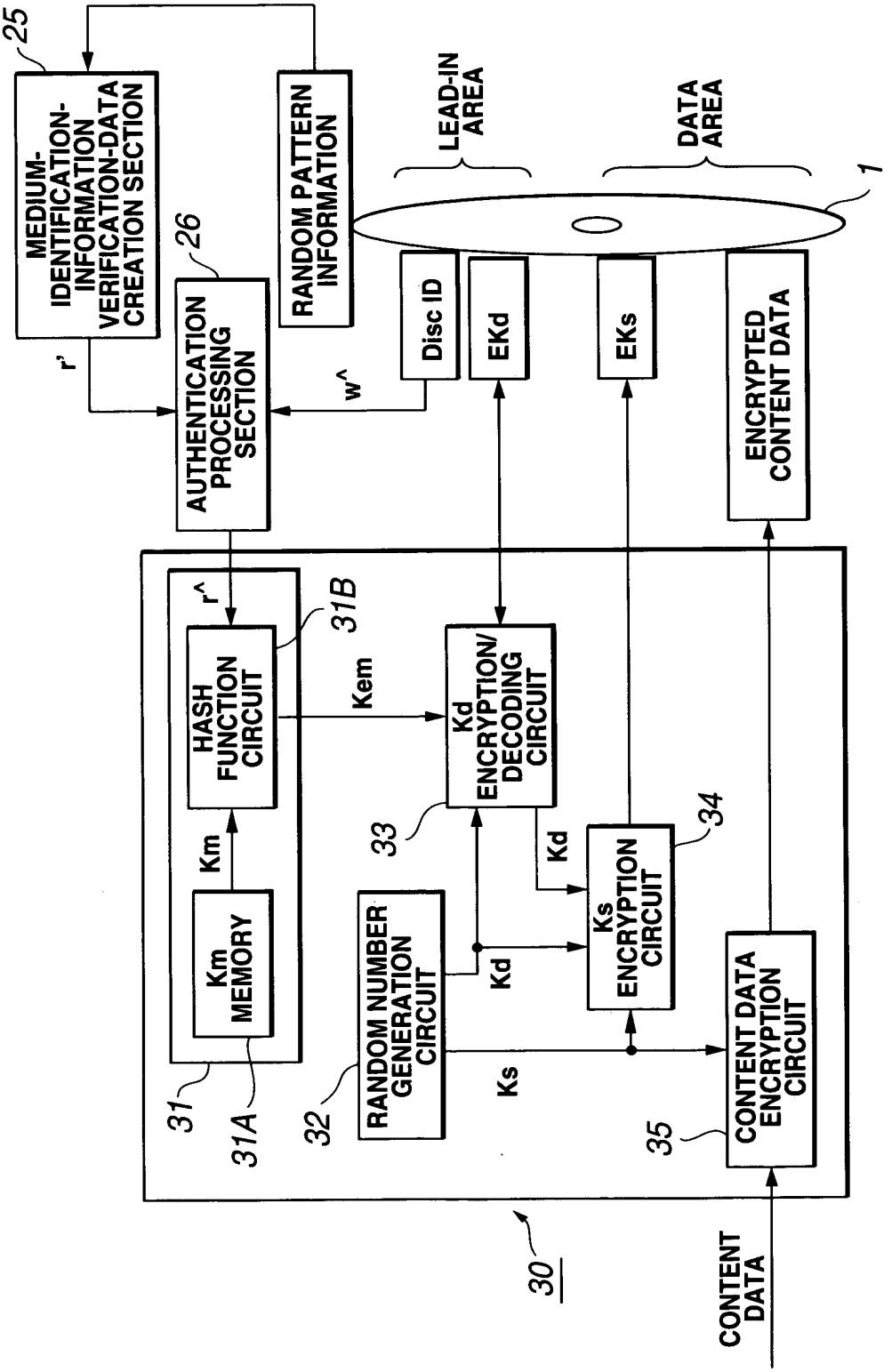
25
MEDIUM-IDENTIFICATION-INFORMATION VERIFICATION-DATA CREATION SECTION
r'
26
AUTHENTICATION PROCESSING SECTION
w^
RANDOM PATTERN INFORMATION
LEAD-IN AREA
DATA AREA
1
Disc ID
EKd
EKs
ENCRYPTED CONTENT DATA
r^
31B
HASH FUNCTION CIRCUIT
Kem
Kd ENCRYPTION/ DECODING CIRCUIT
33
Km
Km MEMORY
Kd
Ks ENCRYPTION CIRCUIT
34
RANDOM NUMBER GENERATION CIRCUIT
Kd
Ks
CONTENT DATA ENCRYPTION CIRCUIT
31
31A
32
35
30
CONTENT DATA

FIG.8

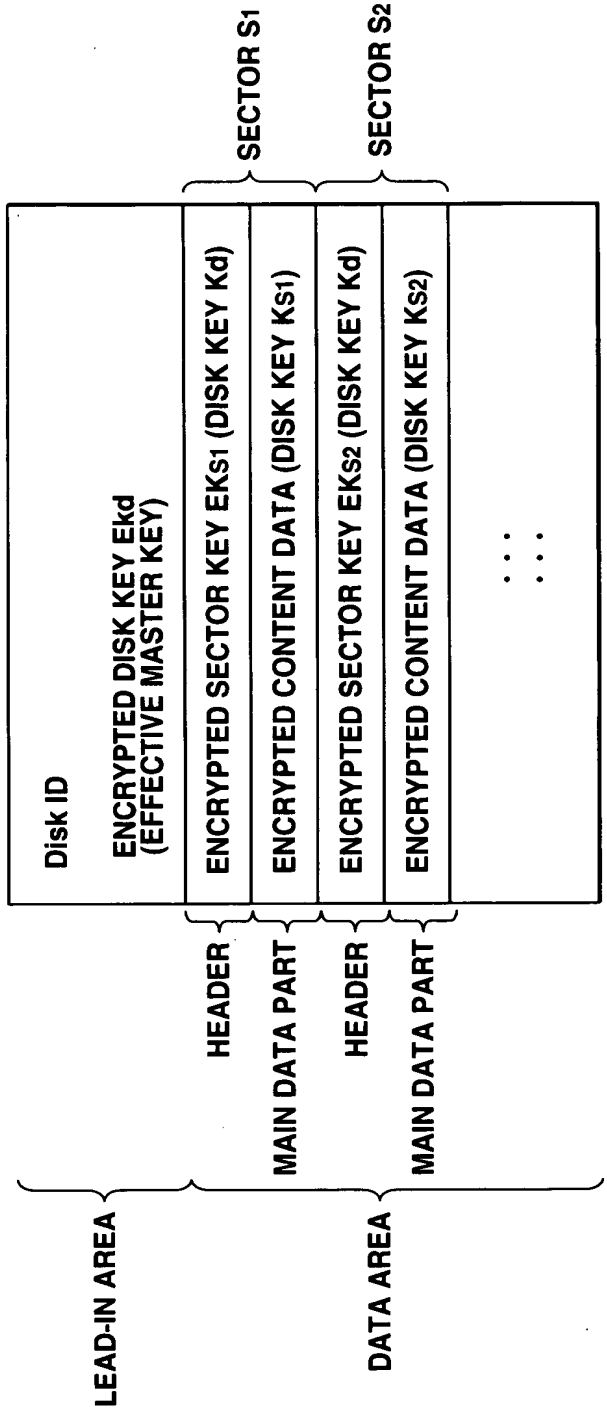
LEAD-IN AREA
DATA AREA
HEADER
MAIN DATA PART
HEADER
MAIN DATA PART
SECTOR S1
SECTOR S2
Disk ID
ENCRYPTED DISK KEY Ekd (EFFECTIVE MASTER KEY)
ENCRYPTED SECTOR KEY EKs1 (DISK KEY Kd)
ENCRYPTED CONTENT DATA (DISK KEY Ks1)
ENCRYPTED SECTOR KEY EKs2 (DISK KEY Kd)
ENCRYPTED CONTENT DATA (DISK KEY Ks2)
. . .
. . .

FIG.9

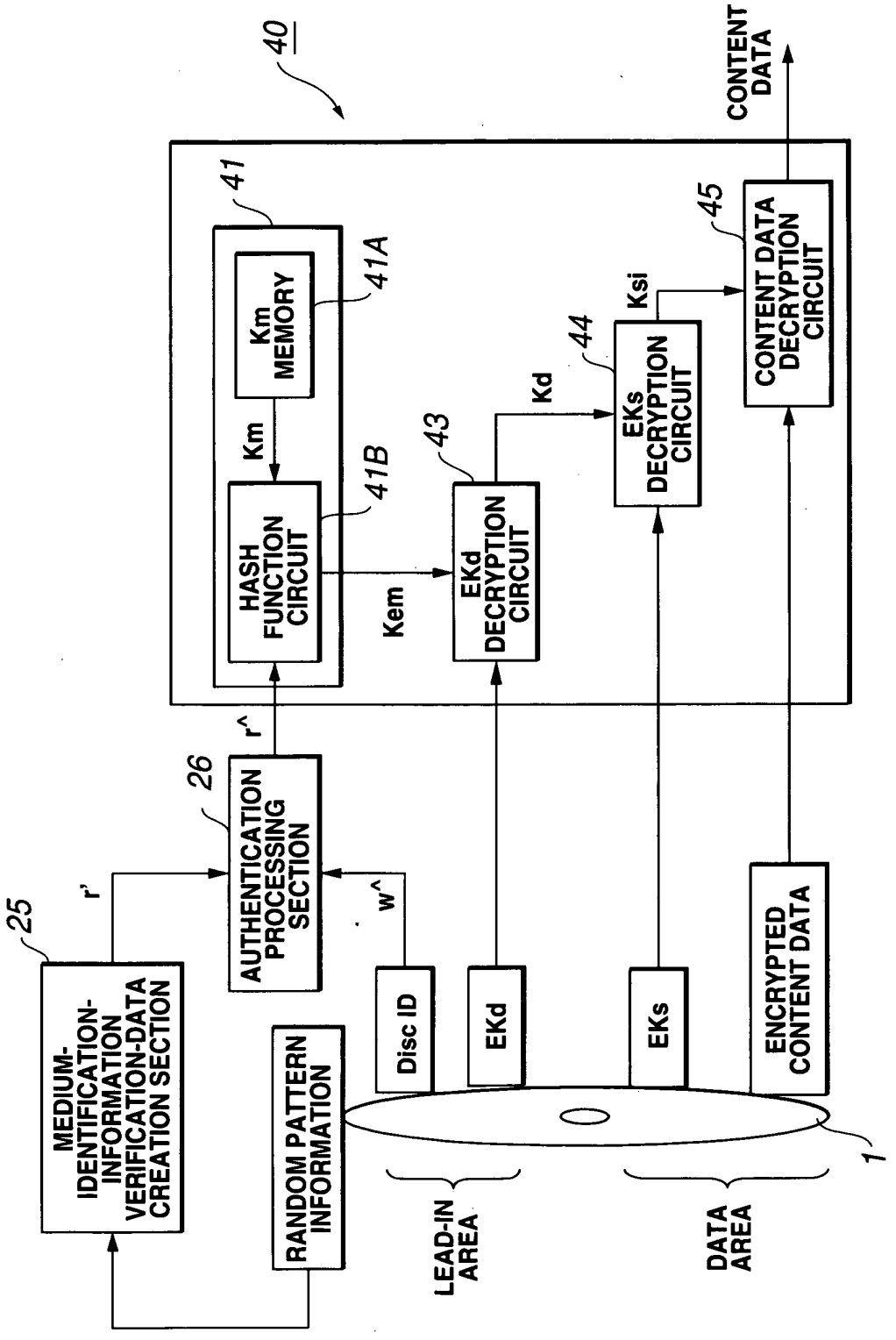
40
CONTENT DATA
41
41A
Km MEMORY
Km
41B
HASH FUNCTION CIRCUIT
Kem
43
EKd DECRYPTION CIRCUIT
Kd
44
EKs DECRYPTION CIRCUIT
Ksi
45
CONTENT DATA DECRYPTION CIRCUIT
r^
26
AUTHENTICATION PROCESSING SECTION
w^
r'
25
MEDIUM-IDENTIFICATION-INFORMATION-VERIFICATION-DATA CREATION SECTION
RANDOM PATTERN INFORMATION
Disc ID
EKd
EKs
ENCRYPTED CONTENT DATA
1
LEAD-IN AREA
DATA AREA

FIG.10

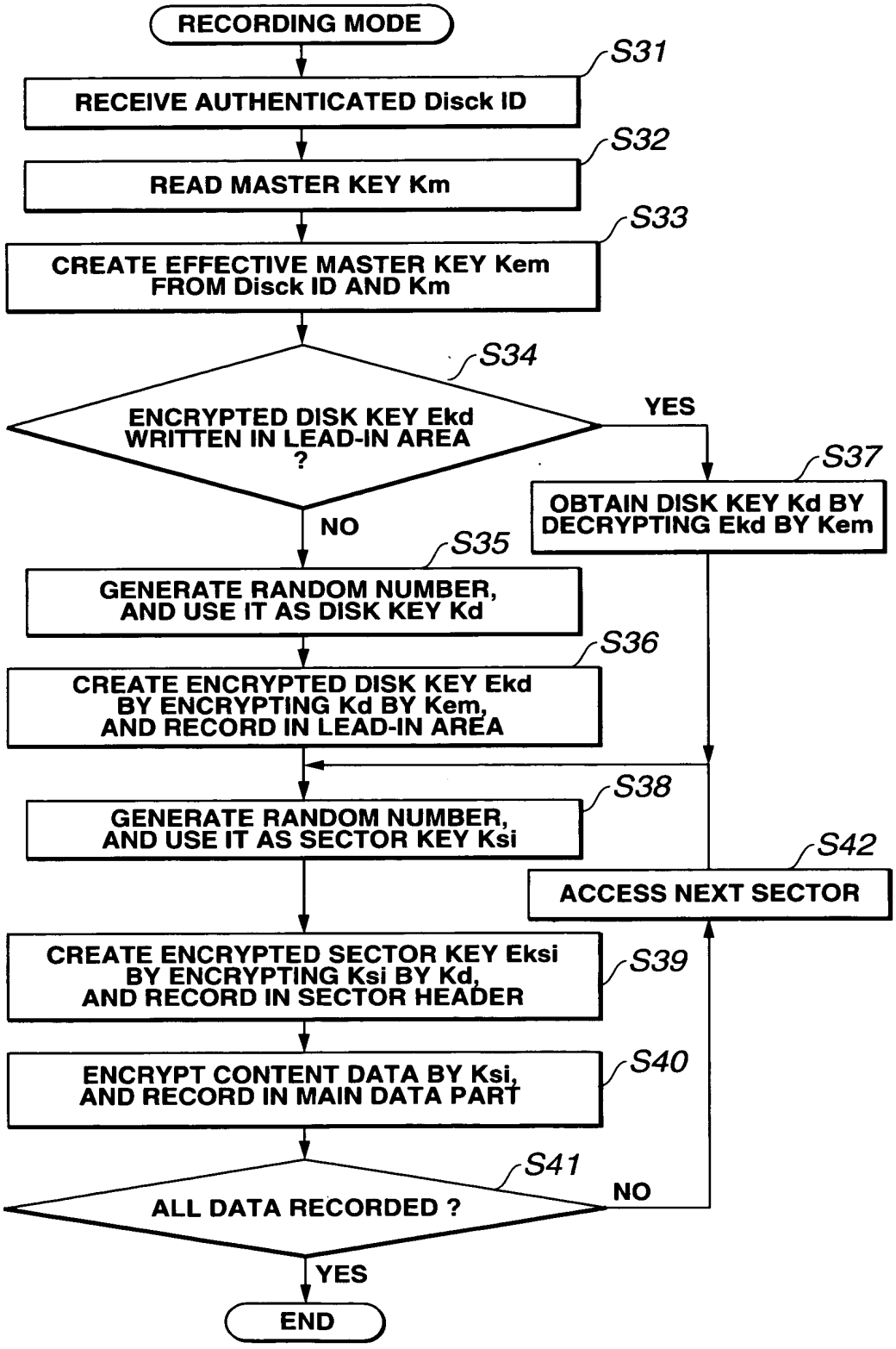
RECORDING MODE
S31
RECEIVE AUTHENTICATED Disck ID
S32
READ MASTER KEY Km
S33
CREATE EFFECTIVE MASTER KEY Kem FROM Disck ID AND Km
S34
ENCRYPTED DISK KEY Ekd WRITTEN IN LEAD-IN AREA ?
YES
NO
S37
OBTAIN DISK KEY Kd BY DECRYPTING Ekd BY Kem
S35
GENERATE RANDOM NUMBER, AND USE IT AS DISK KEY Kd
S36
CREATE ENCRYPTED DISK KEY Ekd BY ENCRYPTING Kd BY Kem, AND RECORD IN LEAD-IN AREA
S38
GENERATE RANDOM NUMBER, AND USE IT AS SECTOR KEY Ksi
S42
ACCESS NEXT SECTOR
CREATE ENCRYPTED SECTOR KEY Eksi BY ENCRYPTING Ksi BY Kd, AND RECORD IN SECTOR HEADER
S39
ENCRYPT CONTENT DATA BY Ksi, AND RECORD IN MAIN DATA PART
S40
S41
ALL DATA RECORDED ?
NO
YES
END

FIG.11

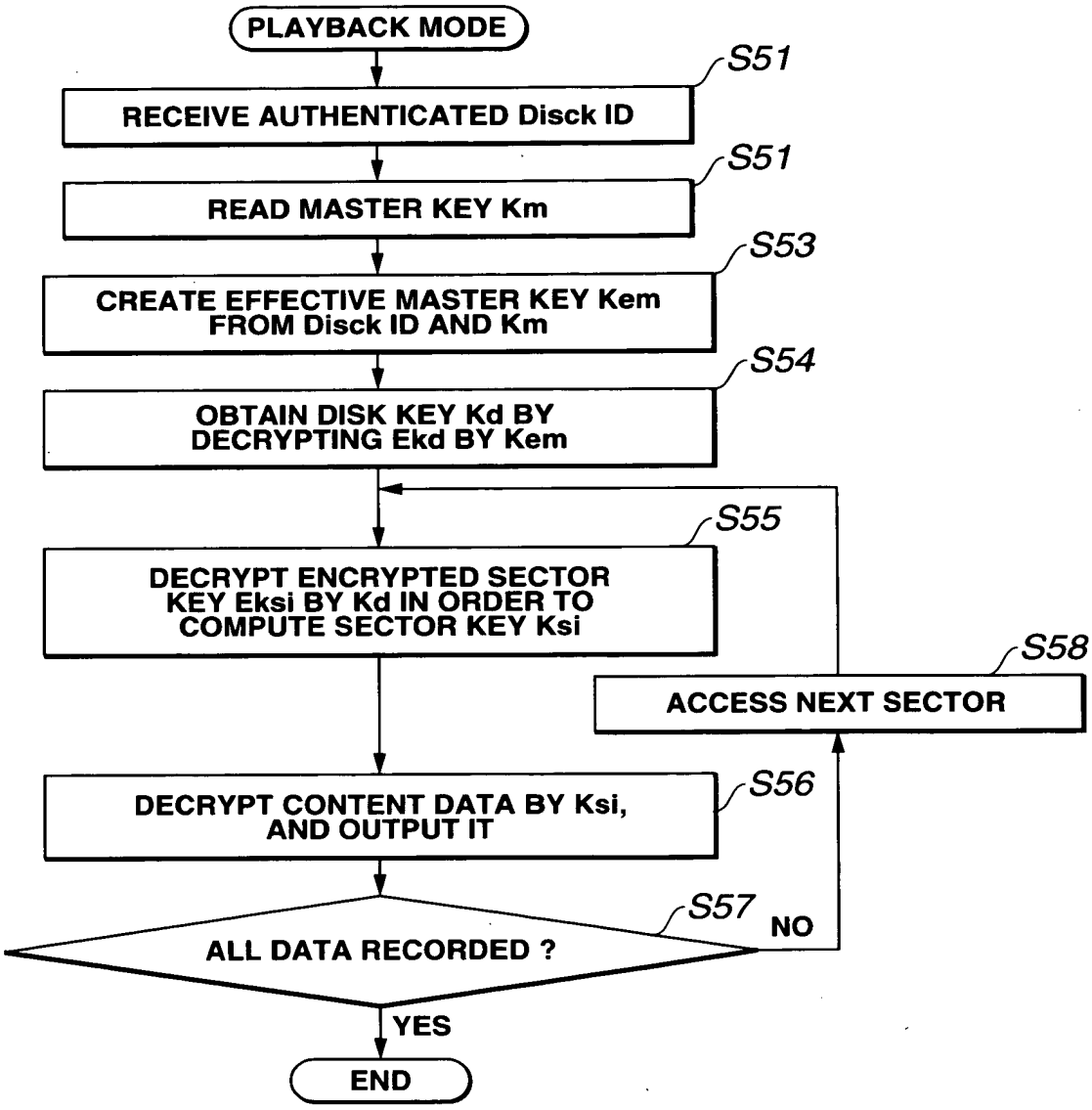
PLAYBACK MODE
S51
RECEIVE AUTHENTICATED Disck ID
S51
READ MASTER KEY Km
S53
CREATE EFFECTIVE MASTER KEY Kem FROM Disck ID AND Km
S54
OBTAIN DISK KEY Kd BY DECRYPTING Ekd BY Kem
S55
DECRYPT ENCRYPTED SECTOR KEY Eksi BY Kd IN ORDER TO COMPUTE SECTOR KEY Ksi
S58
ACCESS NEXT SECTOR
S56
DECRYPT CONTENT DATA BY Ksi, AND OUTPUT IT
S57
ALL DATA RECORDED ?
NO
YES
END

FIG.12

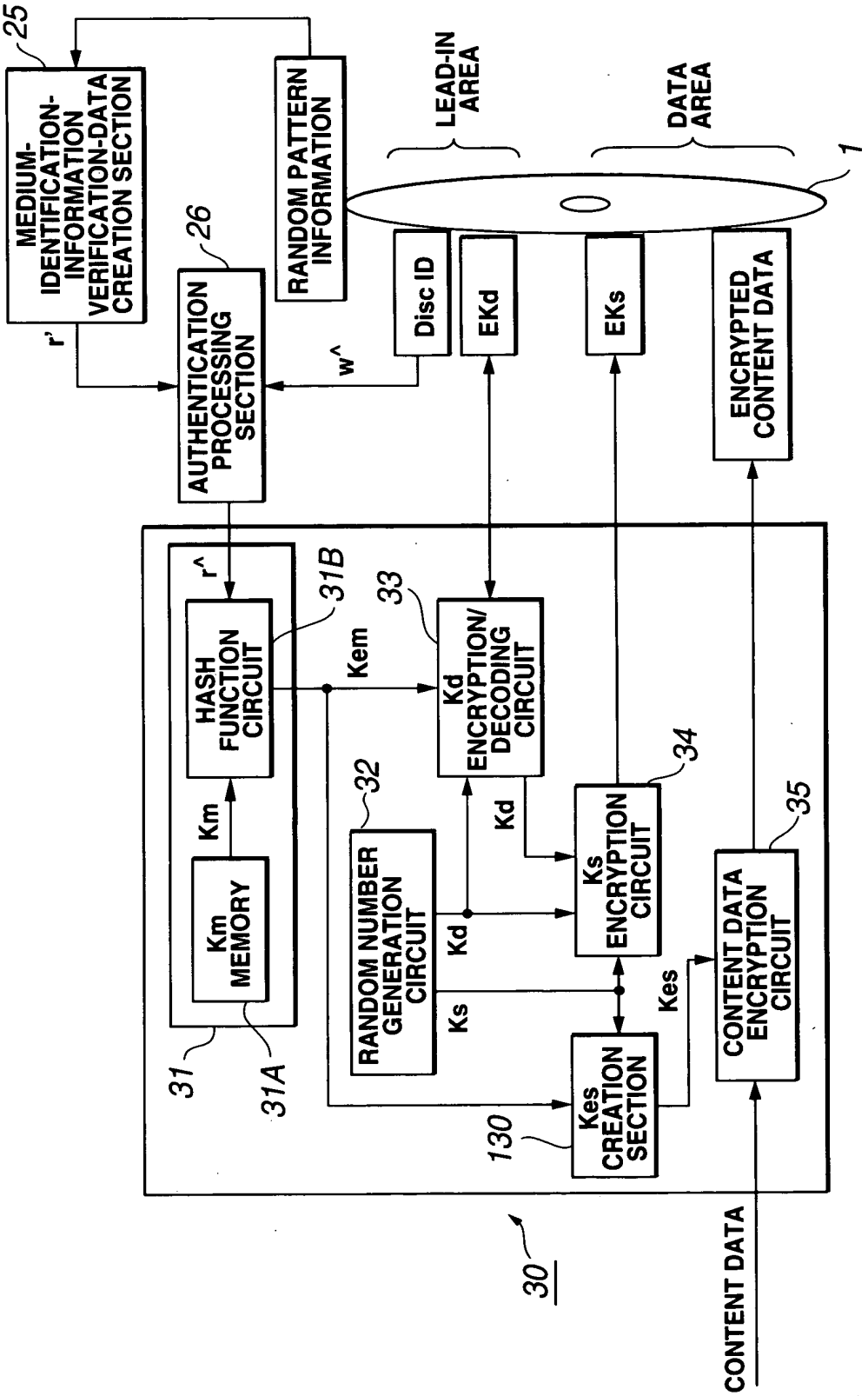
25
MEDIUM-IDENTIFICATION-INFORMATION VERIFICATION-DATA CREATION SECTION
r'
26
AUTHENTICATION PROCESSING SECTION
w^
RANDOM PATTERN INFORMATION
LEAD-IN AREA
DATA AREA
1
Disc ID
EKd
EKs
ENCRYPTED CONTENT DATA
r^
HASH FUNCTION CIRCUIT
31B
Kem
33
Kd ENCRYPTION/ DECODING CIRCUIT
Km
Km MEMORY
32
RANDOM NUMBER GENERATION CIRCUIT
Kd
Ks
34
Ks ENCRYPTION CIRCUIT
Kes
35
CONTENT DATA ENCRYPTION CIRCUIT
31
31A
130
Kes CREATION SECTION
30
CONTENT DATA

FIG.13

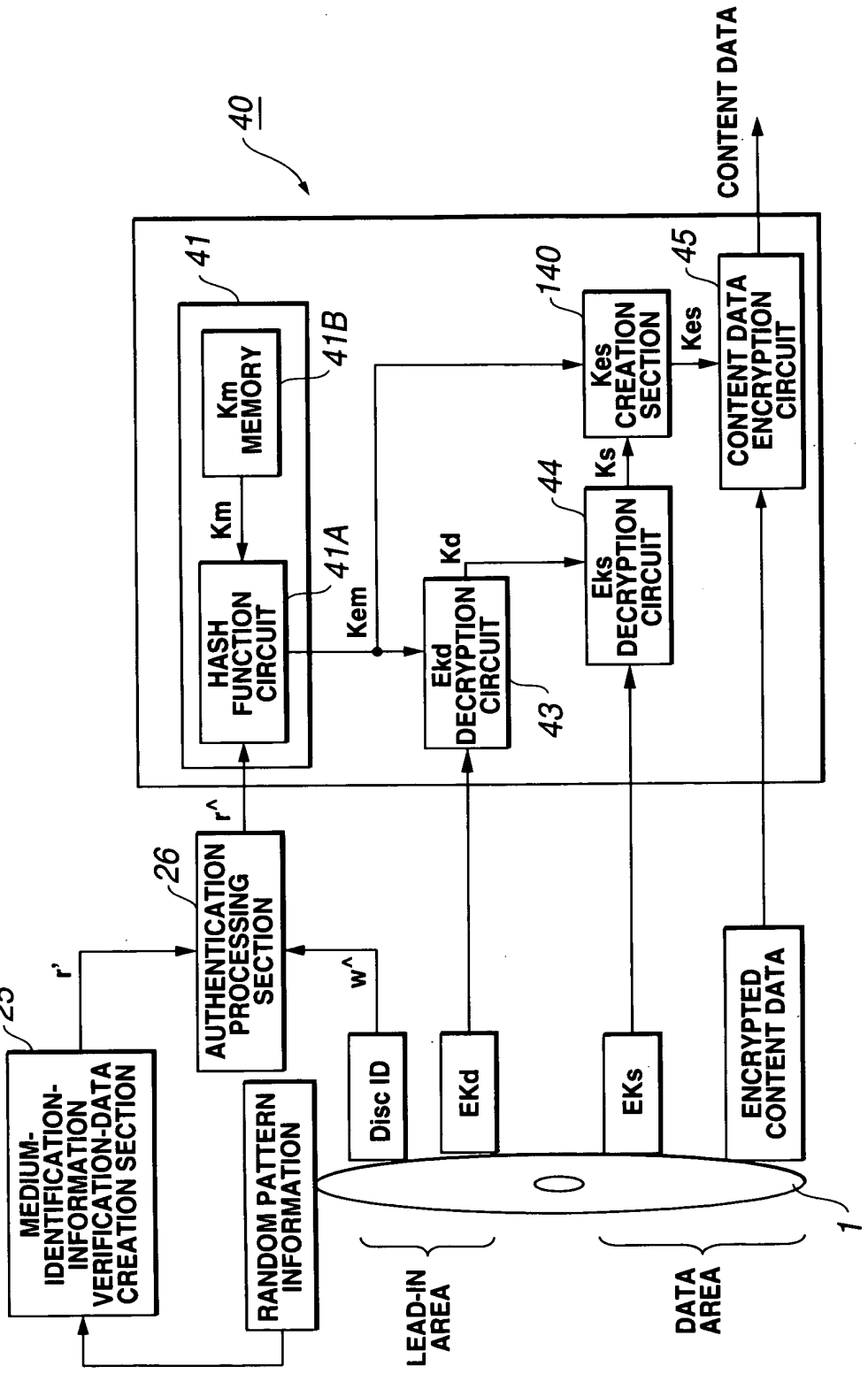
40
CONTENT DATA
41
Km MEMORY
41B
HASH FUNCTION CIRCUIT
41A
Km
Kem
Kd
Ekd DECRYPTION CIRCUIT
43
140
Kes CREATION SECTION
Kes
45
CONTENT DATA ENCRYPTION CIRCUIT
44
Ks
Eks DECRYPTION CIRCUIT
r^
26
AUTHENTICATION PROCESSING SECTION
r'
25
MEDIUM-IDENTIFICATION-INFORMATION-VERIFICATION-DATA CREATION SECTION
w^
RANDOM PATTERN INFORMATION
Disc ID
EKd
EKs
ENCRYPTED CONTENT DATA
1
LEAD-IN AREA
DATA AREA

FIG.14

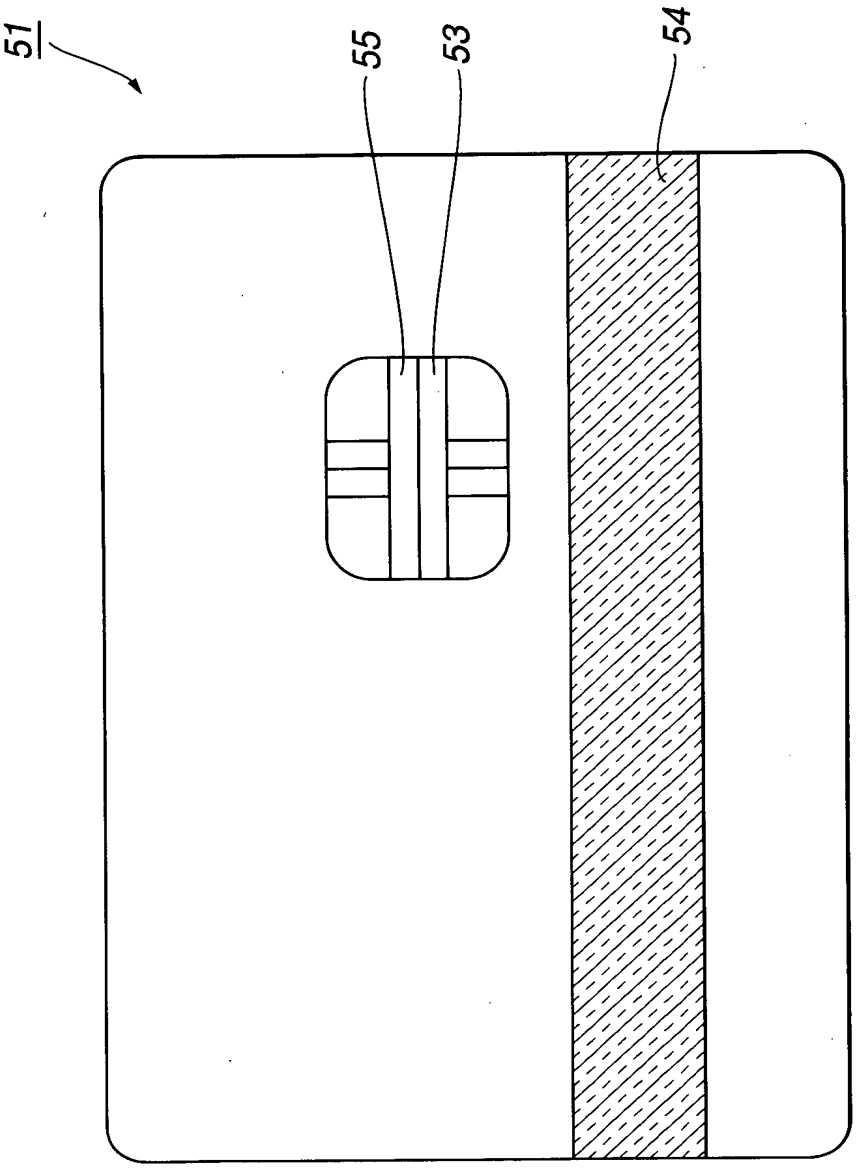

FIG.15